UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/739,839	12/20/2000	Yusuke Kawasaki	1080.1088/JDH	3883

21171 7590 01/28/2009

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
01/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/739,839	KAWASAKI ET AL.	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-11,13-23,25-29 and 31-36* is/are pending in the application.

4a) Of the above claim(s) *11,13-17,19,29 and 31-36* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-10,18,20-23 and 25-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 11/19/2008

DETAILED ACTION

Election/Restrictions

Applicant's election without traverse of claims 1-4, 6-10, 18, 20-23, and 25-28 in the reply filed on 11/19/2008 is acknowledged.

Claims 11, 13-17, 19, 29, and 31-36 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected invention, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 11/19/2008.

Response to Arguments

Applicants' arguments filed 7/7/2008 have been fully considered but are moot in view of the new grounds of rejection presented below.

Claims 1-4, 6-10, 18, 20-23, and 25-28 have been examined.

All objections and rejections not set forth below have been withdrawn.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification fails to provide proper support for the newly claimed limitation of "the second clock at a higher speed than a speed of the first clock…**so that the ciphering patterns vary depending on clock speed**". For further details, see the rejection of the claims under 35 USC 112 1st Paragraph below.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-4, 6-10, 18, 20-23, and 25-28 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. In this case, the newly claimed limitation of the ciphering patterns varying depending on clock speed does not appear to have support in the specification. While the examiner can find support for the higher rate of the second clock so that more complicated ciphering patterns can be used, the examiner cannot find support for the ciphering patterns varying depending on clock speed. Further, the examiner cannot find support in the portion of the specification which the applicant has pointed to as showing support. As such, the ordinary person skilled in the art would be unable to determine whether the applicants were in possession of the invention, as claimed, at the time of application. Therefore, the claims are rejected for failing to meet the written description requirement of 35 USC 112 1st Paragraph.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 6-10, 21-22, and 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Taguchi et al. (U.S. Patent Number 5,915,025) hereinafter referred to as Taguchi, and further in view of Curran et al. (U.S. Patent Number 4,525,599) hereinafter referred to as Curran, further in view of Schneier (Applied Cryptography), further in view of Milhaupt et al. (U.S. Patent Number 5,706,445) hereinafter referred to as Milhaupt, and further in view of Robbins (US Patent Number 4,628,358).

Regarding claims 1 and 20, Taguchi disclosed an internal circuit (See Taguchi Fig. 31 the Elements within Element 150) comprising a CPU executing programs, said CPU is supplied with a first clock and executes the programs synchronously with the supplied first clock (Element 151), at least one internal device having a predetermined function (Elements 152-157) and a bus line extending internally of the internal circuit (See connection from 153 and 154 to 160, and Col. 25 Lines 44-51, Col. 21 Lines 18-28, Col. 10 Lines 50-62, and Col. 9 Lines 49-65 especially lines 61-63) and connecting said CPU to said internal device (See connection from 151 to 153 and 154) the bus line comprising an externally extending portion extending externally of said internal circuit (See connection from 153 and 154 to 160, and Col. 25 Lines 44-51, Col. 21 Lines

18-28, Col. 10 Lines 50-62, and Col. 9 Lines 49-65 especially lines 61-63) and transferring an address and data (See Col. 8 Lines 55-59), wherein said internal circuit includes at least one internal memory as an internal device (See Taguchi Fig. 31 Element 155 and Col. 13 Paragraphs 2-4 wherein it is disclosed that the key supply stores keys and retrieves keys upon request. Further see Taguchi Col. 2 Line 55 Col. 3 Line 55 wherein it was disclosed that processors had cache memory), the internal circuit including selection means for determining ciphering patterns (See Taguchi Col. 4 Paragraph 4 and Col. 22 Paragraph 3).

Taguchi further disclosed an external circuit (Elements 161-166) provided externally of the internal circuit and connected with the externally extending portion of said bus line (See all elements below 160) and including at least one external device having a predetermined function (Elements 161-166), wherein said external circuit includes at least one external memory as an external device (See Taguchi Fig, 31 Element 161 and Col. 8 Lines 33-36 wherein it was disclosed that the external storage was RAM (Random Access Memory)).

Taguchi also disclosed that the internal circuit comprises a ciphering section (Element 153) interposed at an entrance to an external side of said internal circuit (See connection from 153 to 160, and Col. 25 Lines 44-51, Col. 21 Lines 18-28, Col. 10 Lines 50-62, and Col. 9 Lines 49-65 especially lines 61-63) and ciphering the data on the bus line by ciphering patterns according to a plurality of regions divided from an address space allotted to entirety of said at least one external device (See Col. 8 Paragraph 5).

However, Taguchi failed to disclose the ciphering of the address. Curran, on the other hand, teaches that software can be protected from illegal copying by encrypting the addresses of the data being accessed in order to provide a non-sequential ordering of the data in memory as

well as encrypting the data stored therein (See Col. 1 Paragraph 5 – Col. 2 Paragraph 1 and Col. 3 Paragraph 3). It also would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Curran to the invention of Taguchi in order to encrypt the addresses as well as the data on the external bus. This would have been obvious because the ordinary person skilled in the art would have been motivated to further protect the software and other data stored external from the data processor from illicit access.

Further, Taguchi failed to disclose that the selection means included a program stored in internal memory for determining the ciphering patterns. Schneier teaches that any encryption algorithm can be implemented in software in order to provide flexibility, portability, ease of use, and ease of upgrade (See Schneier Page 225 Lines 24-43). It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the software protection apparatus of Taguchi and Curran by implementing the encryption method selection means 157 in software. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide flexibility, portability, ease of use, and ease of upgrade of the selection means. It further would have been obvious that the software would have been stored in memory in the protection apparatus in order for it to have been used by the protection apparatus (See Taguchi Fig. 31 Element 157).

Taguchi further failed to disclose using separate clocks with the encryption clock being set at a higher frequency than the processor clock. However, Taguchi did disclose that when encrypted software was input to the system at the CD-ROM drive (See Taguchi Fig. 31) the decryption means had to decrypt the software and then the encryption means had to encrypt the software and store the software in memory before the processor could access the software (See

Taguchi Col. 10 Paragraph 1). Milhaupt teaches that reducing the clock rate to the processor during times when the processor is not being used can dramatically reduce the power consumed by a processor (See Millhaupt Fig. 5 and Col. 8 Lines 52-53 and Col. 11 Paragraph 2). It would have been obvious to the ordinary person skilled in the art to employ the teachings of Milhaupt in the system of Taguchi by providing each portion of the device with a separate clock which can be throttled back when the portion is idle, and further to throttle back the clock of the processing means when the processing means is idle and the encryption/decryption means is active. This would have been obvious because the ordinary person skilled in the art would have been motivated to reduce the power consumed by the data processor while the processor was idle and waiting for the software to be re-encrypted and stored in memory.

Taguchi further failed to disclose the ciphering pattern varying depending on clock speed, but did disclose varying the ciphering pattern. Robbins teaches a system for determining encrypting patterns using a random number generator which is clocked by dividing down vertical synchronizing pulses such that the encrypting pattern varies depending on the clock (See Robbins Col. 6 Line 56 - Col. 7 Line 23). It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Robbins in the cipher varying system of Taguchi by using a clocked pseudo-random generator to generate the varying cipher patterns. This would have been obvious because the ordinary person skilled in the art would have been motivated to further secure the encrypted data.

Taguchi also failed to specifically state that the processing means was provided with cache memory, but Taguchi did imply that the cache memory was there (See Taguchi Col. 2 Line 55 Col. 3 Line 55). However, it was well known in the art at the time of invention that

processors accessed data directly from cache memory and external storage, such as RAM, accessed the data from the cache memory (See Taguchi Col. 2 Line 55 Col. 3 Line 55). It therefore would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was known in the art at the time of invention to the processing system of Taguchi by storing data to be input and output by the processing means in cache memory. This would have been obvious because the ordinary person skilled in the art would have been motivated to decrease the access time to the data. In this combination, illicit access to the data in the cache would be prevented because the data sent out of the internal circuit from the cache would be encrypted (See Taguchi Col. 8 Paragraph 5).

Even further still, Taguchi failed to specifically disclose that the system bus comprised both an address bus and a data bus. It was further well known in the art at the time of invention that busses comprised an address bus, data bus, and control bus and therefore it would have been obvious to the ordinary person skilled in the art for the system bus of Taguchi to incorporate all three as well.

Regarding claims 2 and 21, Taguchi, Curran, Schneier, Millhaupt, and Robbins further disclosed that the ciphering patterns include at least one pattern in which neither the address nor the data is enciphered (See Taguchi Col. 14 Paragraph 1 and Col. 20 Paragraph 45-56 wherein the encryption being performed was a basic XOR and the encryption keys were chosen randomly. In this case, that the random key could be a string of all zeros, and XORing data with all zeros does not encrypt the data.).

Regarding claims 3 and 22, Taguchi, Curran, Schneier, Millhaupt, and Robbins disclosed that the external circuit includes a plurality of external devices (See Taguchi Fig. 31 Elements

161-166), and said ciphering section performs ciphering using ciphering patterns according to said plurality of external devices, respectively (See Taguchi Fig. 15).

Regarding claims 6 and 25, Taguchi, Curran, Schneier, Millhaupt, and Robbins disclosed that the ciphering pattern determination means for recognizing a constitution of said external circuit and determining a ciphering pattern of said ciphering section according to the constitution of said external circuit (See Taguchi Col. 9 Paragraph 5 – Col. 10 Paragraph 1).

Regarding claims 7 and 26, Taguchi, Curran, Schneier, Millhaupt, and Robbins disclosed that the said ciphering section ciphers the address and the data on said bus line by ciphering patterns according to the plurality of regions divided from the address space allotted to the entirety of said no less than one external device and according to application programs executed by said CPU (See Taguchi Fig. 15 and Col. 8 Lines 55-63).

Regarding claim 8, Taguchi, Curran, Schneier, Millhaupt, and Robbins disclosed a deciphering section connected to the externally extending portion of said bus line, and returning the ciphered address and the data on the bus line to an address and data which are not ciphered (See Taguchi Fig. 31 Element 154 and Col. 10 Lines 25-27).

Regarding claims 9 and 27, Taguchi, Curran, Schneier, Millhaupt, and Robbins disclosed ciphering pattern change means for changing a ciphering pattern whenever a predetermined initialization operation is carried out for one of the plurality of regions divided from the address space allotted to the entirety of said at least one external device (See Taguchi Fig. 11, Fig. 13, and Fig. 15).

Regarding claims 10 and 28, Taguchi, Curran, Schneier, Millhaupt, and Robbins disclosed that the ciphering section adopts a ciphering pattern in which ciphered data is changed

according to the address, for one of the plurality of regions divided from the address space allotted to the entirety of said at least one external device, to thereby cipher the data (See Taguchi Fig. 11, Fig. 13, and Fig. 15).

Regarding claim 18, Taguchi, Curran, Schneier, Millhaupt, and Robbins disclosed that the internal circuit holds a ciphering pattern adopted by said ciphering section (See Taguchi Fig. 31 Element 155), the processing apparatus further comprises a tamper detection section detecting tamper, and ciphering pattern destruction means for destroying the ciphering pattern held in said internal circuit in response to tamper detection made by said tamper detection section (See Taguchi Col. 9 Paragraph 2).

Claims 4 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Taguchi, Curran, Schneier, Millhaupt, and Robbins as applied to claims 1 and 20 respectively above, and further in view of IBM (IBM Technical Disclosure Bulletin 19800601).

The combination of Taguchi, Curran, Schneier, Millhaupt, and Robbins disclosed the use of random number in generating keys (See Taguchi Col. 14 Lines 4-6), but the combination of Taguchi, Curran, Schneier, Millhaupt, and Robbins failed to disclose any information regarding times when the external bus was not being used.

IBM teaches that memory can be tested by generating random addresses, storing random data to the random addresses, and then checking that the generated data and the stored data are consistent.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of IBM in the combination of Taguchi and Curran and Schneier and Millhaupt in order to test the memory when the external bus was not in use. This

would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that the external memory was working properly, thus ensuring data integrity.

Conclusion

Claims 1-4, 6-10, 18, 20-23, and 25-28 have been rejected.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431